PRIVACY IMPACT ASSESSMENT

Submit in *Word format* electronically to: Judy Hutt (hutt.judy@epa.gov)
Office of Environmental Information

System Name: EPA Personnel Access and Security System (EPASS)		
Preparer: Bridget C. Shea	**Office:** Security Management Division, OARM	
Date: 19 June 2006	**Phone: (202) 564-5441**	
This project is in the following stage(s):		
Definition ☒	Development/Acquisition ☒	Implementation ☐
Operation & Maintenance ☐	Termination ☐	

I. Data in the System

1. Generally describe what information will be collected in the system.
The information that will be collected or stored in EPASS is that required to comply with the Personal Identity Verification (PIV) mandates set forth in Homeland Security Presidential Directive (HSPD) 12 and implementing guidance. The mandated information includes the EPA employee's or contractor's name, EPA's employee number, the contractor unique generated number, two fingerprint templates, digital photograph, Cardholder Unique Identifier (CHUID), Federal Agency Smart Credential Number (FASC-N) and the EPASS badge serial number.

2. What are the sources and types of the information in the system?
OASIS personnel security module (individual's demographic and background investigation information), fingerprint biometrics, digital photograph (EPASS enrollment workstation), and the cardholder unique identifier (CHUID).

3. How will the data be used by the Agency?
The data will be used in the process of requesting, authorizing, issuing, maintenance, and disposal of all EPASS badges.

4. Why is the information being collected? (Purpose)
This information is being collected pursuant to the requirements of HSPD-12 and implementing guidance which mandate that all Federal agencies issue PIV badges to all employees and certain non-Federal workers.

II. Access to the Data

1. Who will have access to the data in the system (*internal and external parties*)? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?
Data access will be granted only to those Office of Administrative Services (OAS) employees and certain contractor staff who are authorized and have an official need to know. For example, the EPASS System Administrator will have total data access, while the authorized OAS staff who serves as the operators of the enrollment workstations will have limited data access for the individual being processed during the enrollment and issuance process. Contractors with access are governed by the requirements of EPA's Policies for Information Resources Management (EPAAR 1552.211-79 October 2000). Further, contractors are responsible for operating under the Enterprise Technology Services Division (ETSD) Operations Directives Manual.

2. What controls are in place to prevent the misuse of data by those having authorized access?
Only those OAS staff members who have the proper authorization and roles in EPASS are allowed to access any of the subject information. Each individual who has access privileges to EPASS will use the PIV Card Public Key Infrastructure (PKI) authenication certificate to first log into the system. This procedure will activate the auditing log

that is used to track and report their activities when using EPASS. This auditing log will be regularly reviewed for anomalous patterns in conformance with guidelines for such audits set forth in NIST SP-800-53 and NIST AP 800-53A.
In addition, those individuals authorized to view EPASS data will have their access privileges strictly governed by the principles of "separation of duties," "least privilege", and "minimum data required", in accordance with OMB Circular A-130 and as set forth in NIST special publications, particularly NIST SP 800-53.
Furthermore, EPA will conduct a mandatory training program for all EPASS authorized users, emphasizing the sensitive nature of the data, the mandatory security practices and procedures that all authorized users must follow, and the consequences for not following those practices and procedures.

3. Do other systems share data or have access to data in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface? (i.e., *System Administrators, System Developers, System Managers)*
No, EPASS will pull information from the OASIS personnel security module. Information within EPASS will not be shared with any system outside of its boundaries.

4. Will other agencies, state or local governments share data or have access to data in this system? *(Includes any entity external to EPA.)*
No.

5. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? If yes, how is notice given to the individual? *(Privacy policies must clearly explain where the collection or sharing of certain information may be optional and provide users a mechanism to assert any preference to withhold information or prohibit secondary use.*)
The information provided by each individual is necessary for compliance with HSPD-12 and its implementing guidance, and to issue an EPASS badge, which is required for employment at EPA; withholding such requested information will affect job placement, employment prospects, or continued employment at the Agency. Notice of EPASS badge holders' privacy rights is provided in the application form, the Notice of Applicant Privacy Rights and Responsibilities and relevant Agency Privacy Act System of Records Notices.

III. Attributes of the Data

1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed.
The information is required for HSPD-12 compliance in general and specifically, required for the issuance of compliant PIV cards.

2. If data are being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain.
EPASS does not consolidate data. However, all EPASS data is protected by the implementation of the security controls specified in NIST SP 800-53 for a system with a FIPS 199 category of MODERATE."

3. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
Yes, only OAS staff who have the proper authorization and roles in EPASS are permitted access to any of the system information. Further, each authorized OAS staff member is assigned a role that gives him or her access to only the limited data required to perform his/her job. Each OAS staff member who has access to EPASS will use his/her PKI authentication certificate to log onto the system. EPASS auditing logs are used to enhance the supervision checks and audit trails to report all access and operation of the system.

4. How will data be retrieved? Can it be retrieved by personal identifier? If yes, explain. (*A personal identifier is a name, Social Security Number, or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual.)*
The data will normally be retrieved by the user's name. In some cases EPASS' workflow engine will use both the user's name and his or her unique number (employee or contractor number) for retrieval.

5. What achievements of goals for machine readability have been incorporated into this system? Where is the policy stated? *(Machine readable technology enables visitors to easily identify privacy policies and make an informed choice about whether to conduct business with that site.)*
Because EPASS is an internal control system central to the functioning of the HSPD-12 PIV program, there is an opportunity to achieve any of the E-Government Act goals with regard to collecting data from the public via non-paper collection vehicles. Moreover, EPASS is a system to be used only by personnel authorized to operate portions or components of the system. If an unauthorized access is attempted, the EPASS screen will display a warning message stating the policy for access.

IV. Maintenance of Administrative Controls

1. Has a record control schedule been issued for the records in the system? If so, provide the schedule number. What are the retention periods for records in this system? What are the procedures for eliminating the records at the end of the retention period? *(You may check with the record liaison officer (RLO) for your AA-ship, Tammy Boulware (Headquarters Records Officer) or Judy Hutt, Agency Privacy Act Officer, to determine if there is a retention schedule for the subject records.*)
No. NARA has not yet issued the guidelines for retaining these records.

2. While the data are retained in the system, what are the requirements for determining if the data are still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
The requirement for checking the accruacy of the data in EPASS is to perform periodic checks from the data obtained from the authoritative data source, the OASIS personnel security module. Data will be cross-checked for accuracy and validity.

3. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
No

4. Does the system use any persistent tracking technologies?
No.

5. Under which System of Records (SOR) notice does the system operate? Provide the name of the system and its SOR number if applicable. A list of Agency SOR's are posted at http://www.epa.gov/privacy/notice/. *(A SOR is any collection of records under the control of the Agency in which the data is retrieved by a personal identifier. The Privacy Act Officer will determine if a SOR is necessary for your system.)*
EPA-19 and EPA-41 cover EPASS. Both are currently under revision and awaiting publication in the Federal Register.